

4 (PRT)

107500131

DT04 Rec'd PCT/PTO 25 JUN 2004

ON-CHIP SECURITY METHOD AND APPARATUS

[0001] This application claims the benefit of priority from United States Patent Application Serial No. 60/342,082 filed on December 26, 2001.

5

FIELD OF THE INVENTION

[0002] The present invention relates to the field of application-specific integrated circuits (ASICs) and on-chip BootROM (Boot Read-Only Memory). In particular, the present invention relates to the field of incorporating security features into on-chip BootROM, preferably for use in a mobile device.

10

BACKGROUND OF THE INVENTION

[0003] Many mobile devices, such as cellular telephones, personal digital assistants (PDAs), and other handheld computing and communicating devices, currently perform numerous and complex functions. Such a mobile device may occasionally require resetting of at least a portion of the software used thereon to a known prior state in order to avoid current or potential problems. Typically, a mobile device comprises a reset switch, or other equivalent means known in the art, which a user can actuate in order to initiate a reset process.

15

[0004] It has been observed that some existing ASIC processors for mobile devices may be breached through their serial port line after a reset process has been initiated. An external reset switch typically controls a reset circuit in the mobile device. When the reset switch is actuated, the reset circuit closes, sending a signal, or reset command, to the ASIC to reset. When the reset switch is released and the reset circuit opens, instructions stored in internal BootROM are executed and the BootROM instructs the ASIC to poll a serial port, which can be connected to a personal computer, for activity.

20

25

[0005] If there is serial port activity, this usually indicates that there is new code to be downloaded. This new code may be stored in memory on a personal computer, or may be transmitted via the personal computer from another source and may comprise, for example, a new version of code to be executed in the mobile

30

device. Typically, program code in the BootROM will jump to a routine for downloading the new code via the serial port into internal SRAM. Once downloading is complete, the program code in BootROM will jump to the beginning of the downloaded new code and begin to execute the downloaded new code. This
5 downloaded new code typically has complete access to other components in the mobile device, such as FLASH memory, in terms of instructions and commands that are permitted. This constitutes a potential security risk, since it can allow anyone to provide new code at the serial port that, once executed, can access and upload programs and data stored in the mobile device's FLASH memory, including
10 confidential and proprietary information. Such access would constitute a security breach.

[0006] It is therefore desirable to provide a security feature in order to reduce the likelihood of occurrence of such a breach.

15 SUMMARY OF THE INVENTION

[0007] It is an object of the present invention to obviate or mitigate at least one disadvantage of previous memory and processor arrangements, particularly those provided for use with handheld or mobile devices.

[0008] A boot method used by an ASIC and memory in a mobile device is
20 described, as well as an apparatus for use in such mobile device. A security feature is provided according to an embodiment of the invention that reduces the likelihood of a security breach, preferably in a situation where a reset of the mobile device has been initiated. The security feature comprises selective polling of the serial port based on the result of a comparison between a value stored on an ASIC, such as in BootROM,
25 and a value stored in FLASH memory.

[0009] A predetermined security value, or password, is stored in a circuit in the mobile device, for example in BootROM. Program code in the BootROM is preferably modified so that a security location within the mobile device's FLASH memory is read prior to polling the serial port for activity. If the value in the security
30 location matches the predetermined security value, then polling of the serial port is not performed. This reduces potential security breaches caused in conventional

arrangements where code may be downloaded from the serial port and executed, which allows anyone to access and upload programs and data in the FLASH memory, including confidential and proprietary information.

[0010] In one aspect of the invention, a predefined memory location, e.g. a security location, in the FLASH memory contains a password, or similar security value. Immediately after a device reset, boot code programmed into the ASIC reads from the security location in the FLASH memory before polling the serial port for activity. If the value read matches the expected password, the boot code jumps directly to the start of FLASH memory and prohibits downloading of a program into system memory via the serial port.

[0011] According to an aspect of the invention, there is provided a boot method for use in a mobile device having FLASH memory storing boot instructions and having a serial port, comprising the steps of: reading contents of a security location in the FLASH memory; comparing the contents of the security location to a predetermined security value; and selectively polling the serial port for activity based on the result of the comparison.

[0012] In a presently preferred embodiment, the polling is performed if the contents of the security location do not match the predetermined security value. The method can further include the step of jumping to a boot location in FLASH memory to execute instructions stored therein. In such a case, the method can further include the step of downloading code into internal SRAM located in the mobile device in response to a detection of serial port activity, as well as the steps of executing an instruction in the downloaded code, and jumping to a boot location in FLASH memory to execute boot instructions stored therein.

[0013] In a boot method according to an embodiment of the invention, the predetermined security value can be stored in a BootROM located in the mobile device. Also, in the boot method, the step of reading is preferably performed in response to a reset command.

[0014] According to another aspect of the invention, there is provided an apparatus for use in a mobile device having a serial port, comprising: a first memory means having a predetermined security value stored therein; a second memory means

having a security location; and a processor in communication with the first and second memory means for comparing the contents of the security location to said predetermined security value, and for selectively polling the serial port for activity based on the result of the comparison.

5 [0015] In a presently preferred embodiment, the first memory means is a Boot Read Only Memory (BootROM), and the second memory means is a FLASH memory. The apparatus can further include a reset means in communication with the processor for initiating a reset process. Preferably, the processor compares contents of the security location and the predetermined security value in response to initiation
10 of a reset process.

[0016] In terms of specific implementations of the apparatus, the first memory means can be located on an ASIC, as can be the processor. The processor can include a microcontrol unit connected to the serial port, and can also include a digital signal processor connected to the second memory means.

15 [0017] Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

20 BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Embodiments of the present invention will now be described, by way of example only, with reference to the attached figures, wherein:

Fig. 1 is a block diagram of a typical ASIC and associated external components operating therewith;

25 Fig. 2 is a block diagram of an ASIC and associated external components operating therewith according to an embodiment of the present invention, incorporating a security feature;

Fig. 3 is a flow diagram of a boot method used by a typical ASIC;

30 Fig. 4 is a flow diagram of a boot method used by an ASIC according to an embodiment of the present invention, having a security feature.

DETAILED DESCRIPTION

[0019] Generally, the present invention provides a method and apparatus for use in a mobile device. A security feature is provided that reduces the likelihood of a security breach, preferably in a situation where a reset of the mobile device has been initiated. A predetermined security value, or password, is stored, for example in BootROM. Program code in the BootROM is preferably modified so that a security location within FLASH memory is read prior to polling the serial port for activity. Polling of the serial port is then selectively performed, depending on the result of a comparison between the stored password and the contents of the security location, or key. In a presently preferred embodiment, if the value in the security location matches the predetermined security value, then polling of the serial port is not performed.

[0020] Fig. 1 is a block diagram of a typical ASIC and associated external components operating therewith. ASIC 2 comprises a digital signal processor (DSP) 4 and a microcontrol unit (MCU) 6. It is well known in the art that the DSP 4 and the MCU 6 are essentially two processors existing in the same integrated circuit and sharing a plurality of resources.

[0021] A reset circuit 8 communicates to the MCU 6 and the DSP 4. An external reset switch 10 controls the reset circuit 8. When the reset switch 10 is actuated, the reset circuit 8 closes, sending a signal, or reset command, to the MCU 6 and the DSP 4 to reset. When the reset switch 10 is released and the reset circuit 8 opens, the MCU 6 executes instructions stored in internal BootROM 14. The reset circuit 8 and the reset switch 10 may be referred to together as comprising a reset means.

[0022] The MCU 6 also communicates with a serial port 12. The serial port 12 can be connected to a personal computer (PC) 11, enabling the PC to communicate with the ASIC 2. Although the invention is described herein as communicating with a PC, the invention is not limited to such an arrangement; any arrangement whereby the required information can be delivered to the processor, i.e. MCU, via the serial port can be used. When the MCU 6 executes instructions stored in the internal BootROM

14 in response to a reset command, the BootROM 14 instructs the MCU 6 to poll the serial port 12 for activity.

[0023] The BootROM 14 is also located on the ASIC 2. The BootROM 14 interfaces unidirectionally with the MCU 6. The DSP 4 and MCU 6 both interface with an external memory interface 16 in order to access an external SRAM 17 and FLASH memory 18. The DSP 4 and MCU 6 also both directly access an internal SRAM 13, or other internal system memory.

[0024] Fig. 2 shows the same ASIC and associated external components as in Fig. 1, but incorporating a security feature according to an embodiment of the present invention.

[0025] A security feature is provided according to an embodiment of the invention that reduces the likelihood of a security breach, preferably in a situation where a reset of the mobile device has been initiated. A predetermined security value, or password, is stored, for example in the BootROM 14. Program code in the BootROM is preferably modified so that a security location within the mobile device's FLASH memory is read prior to polling the serial port for activity.

[0026] Polling of the serial port is then selectively performed, depending on the result of a comparison between the predetermined security value, or stored password, and the contents of the security location. In a presently preferred embodiment, if the value in the security location matches the predetermined security value, then polling of the serial port is not performed, thereby avoiding the potential security risks associated with such polling.

[0027] In an exemplary embodiment, additional code (key reading code) 15 is preferably added to program code stored in the BootROM 14, which is executed therefrom, preferably immediately after a reset. The additional code 15 is used to preferably read a value from a security location 19, or key location, in the FLASH memory 18. The key location 19 is an example of a security location in the FLASH memory 18 in which an expected password can be stored. The term "key" can be used to represent the value stored in the security location, which will be compared to the predetermined security value stored in the BootROM. The security feature can be considered to be a selective polling of the serial port, depending on the result of a

comparison of the key 19 and the expected password. Polling of the serial port is preferably not performed when the FLASH memory 18 has been programmed with the key 19 having a value that matches the predetermined security value, or password, stored in the BootROM 14, and a comparison is made to verify that match.

5 [0028] Fig. 3 is a flow diagram depicting a boot method used by a typical ASIC 2 when a reset is initiated. After initiation of a reset in step 20, program code stored in BootROM 14 initiates polling of the serial port 12 for activity in step 22. If the serial port is connected to a PC 11, then the PC 11 can communicate with the ASIC 2. A determination is made in step 24 as to whether there is any activity on the
10 serial port 12. If there is serial port activity, the program code in BootROM 14 will jump to a routine for downloading code and download such program code, as illustrated in step 26, into internal SRAM 13 via the serial port. Once downloading is complete, the program code in BootROM 14 will jump to the beginning of the downloaded code and begin to execute the downloaded code. A potential security
15 risk in such a configuration is that a downloaded program could upload, or extract, contents of the FLASH memory 18 including confidential and/or proprietary information.

[0029] If, in step 24, it is found that there is no serial port activity, the program code in BootROM 14 waits for a timeout period to elapse, as illustrated in
20 step 28. A current timeout value is determined, for example, by decrementing a count value in a register inside the MCU 6. When the timeout period elapses, the program code in BootROM 14 jumps directly to a boot location in the FLASH memory 18 in step 30 to execute program code starting at the boot location. If the timeout period has not elapsed, then the method returns to step 22 and waits for serial port activity or
25 for the timeout period to elapse. A suitable timeout period can be, for example, 40 msec.

[0030] Fig. 4 shows a flow diagram depicting a boot method according to an embodiment of the present invention providing a security feature as an enhancement over the method in Fig. 3. An ASIC 2 preferably employs this method when a reset is
30 initiated. The BootROM code 14 is preferably modified so that a predefined location,

or security location, in FLASH memory 18 is read prior to polling the serial port 12 for activity.

[0031] Referring to Fig. 4, after a reset is initiated in step 32, the BootROM code 14 preferably reads the contents of the security location in FLASH memory, or the key, 19, in step 34. A determination is then made in step 36 as to whether the key, or the contents of the security location in FLASH memory, matches the password, or predetermined security value, stored in the BootROM. If it is determined that such a match exists, then in step 38, the BootROM code is preferably programmed to jump to the FLASH 18 for execution of instructions in a boot location thereof. Jumping to the boot location in FLASH memory 18 prevents the downloading of a program via the serial port 12 into internal SRAM 13.

[0032] If it is determined in step 36 that the key value does not match the stored password, then the BootROM code 14 polls the serial port 12 for activity in step 40. In step 42, it is determined whether there is any activity on the serial port 12. If in step 42, it is determined that there is activity on the serial port 12, then the method proceeds to step 44. Such a positive determination can be made, for example, when a PC is connected to the serial port. In step 44, the BootROM code 14 jumps to a routine for downloading code into the internal SRAM 13 via the serial port 12. Once this download occurs, the BootROM code 14 jumps to the beginning of the downloaded code.

[0033] If, in step 42, it is found that there is no serial port activity, the program code in BootROM 14 waits for a timeout period to elapse, as illustrated in step 46. A current timeout value is determined, for example, by decrementing a count value in a register inside the MCU 6. When the timeout period elapses, the program code in BootROM 14 jumps directly to a boot location in the FLASH memory 18 in step 38 and the program code execution continues. If the timeout has not elapsed, then the method returns to step 40 and waits for serial port activity or for the timeout period to elapse.

[0034] Although the option of polling the serial port for activity still exists in the flowchart in Fig. 4, this path will be followed only in the absence of a security value that matches the stored password. Programming of a predetermined security

value and a matching value in a security location in FLASH memory is preferably performed during development or production of the mobile device, prior to its commercial sale. It is possible that a malicious individual could try to modify the code following its commercial sale so that the key is not recognised as matching the password, in which case polling of the serial port would occur. However, such a security breach would be difficult to attempt outside of the development phase, once the key reading code 15 has been added to the BootROM code 14. Furthermore, attempting a breach to take advantage of this potential security risk would involve invasive measures not generally known to a layperson.

10 [0035] Although expressions such as security location and memory location are used herein in the singular, this is simply for convenience and one skilled in the art will appreciate that any number of memory locations may be used in order to store a predetermined security value or values. The number of memory locations required can depend on the complexity of the security value and its length, which may affect
15 the selection of the predetermined security value. In terms of physical implementation, such memory locations may be either contiguous or non-contiguous locations linked to one another in some manner known to those skilled in the art, so as to represent, together, a security location, for example.

[0036] In an alternative embodiment, selective polling of the serial port is
20 performed in the case where the value in the security location does match the predetermined security value. Any other suitable comparison scheme or equivalent security feature may be alternatively used in order to regulate the selective polling of the serial port in a mobile device.

[0037] The above-described embodiments of the present invention are
25 intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those of skill in the art without departing from the scope of the invention, which is defined solely by the claims appended hereto.